Williams, E. J., Hinds, J., & Joinson, A. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, *120*, 1-13. https://doi.org/10.1016/j.ijhcs.2018.06.004

International Journal of Human-Computer Studies 120 (2018) 1–13

Contents lists available at ScienceDirect

International Journal of Human-Computer Studies

journal homepage: www.elsevier.com/locate/ijhcs

Exploring susceptibility to phishing in the workplace

Emma J. Williams*, Joanne Hinds, Adam N. Joinson

School of Management, University of Bath, Claverton Down, Bath BA2 7AY, UK

ARTICLE INFO

Keywords:
Phishing
Organisational behavior
Human factors
Cyber security
Employee susceptibility
Social engineering

ABSTRACT

Phishing emails provide a means to infiltrate the technical systems of organisations by encouraging employees to click on malicious links or attachments. Despite the use of awareness campaigns and phishing simulations, employees remain vulnerable to phishing emails. The present research uses a mixed methods approach to explore employee susceptibility to targeted phishing emails, known as spear phishing. In study one, nine spear phishing simulation emails sent to 62,000 employees over a six-week period were rated according to the presence of authority and urgency influence techniques. Results demonstrated that the presence of authority cues increased the likelihood that a user would click a suspicious link contained in an email. In study two, six focus groups were conducted in a second organisation to explore whether additional factors within the work environment impact employee susceptibility to spear phishing. We discuss these factors in relation to current theoretical approaches and provide implications for user communities.

1. Introduction

Organisations are increasingly under threat from attackers attempting to infiltrate their computer systems by exploiting the behaviour of human users (Sasse et al., 2001). One means by which this can be achieved is via targeted, fraudulent emails, which aim to persuade employees to click on malicious links, download malicious attachments or transfer organisational funds or other sensitive information. This practice is commonly known as spear phishing (Workman, 2008). A 2016 Cyber Incident Report (Verizon, 2016) highlighted that over 2,000 organisations experienced a data breach in 2015, with the highest number experienced by organisations in the financial sector (a total number of 795). This same report also showed that approximately 1 in 10 employees of such organisations clicked on links or opened attachments contained within sanctioned phishing email tests.

One way in which organisations attempt to raise awareness of spear phishing emails amongst their staff is through the use of simulated phishing tests. This involves the organisation sending simulated, targeted phishing emails to a number of employees and monitoring the resultant 'click-rate' (i.e., the proportion of employees who click on malicious links within the email). Such emails, whether sent as part of simulated phishing tests or by actual fraudsters, use a range of influence techniques to encourage people to respond quickly and without consideration. This includes instilling a sense of urgency or limited availability and exploiting compliance with authority figures (Atkins and Huang, 2013; Cialdini, 2007; Stajano and Wilson, 2011). Examples of influence techniques used in spear phishing emails are shown in Table 1. When such attacks are successful, they can result in substantial reputational damage, monetary losses or operational impacts for the organisation involved (e.g., Landesman, 2016; Piggin, 2016; Zetter, 2016). It is this threat that has contributed to the rise of anti-phishing training games, formal phishing simulation tests, and interface design initiatives to increase employee awareness and assist in the effective management of phishing risks within the workplace (Abawajy, 2014; Dodge et al., 2007).

Despite an increased focus on training and awareness approaches, a 2016 report produced by security training firm PhishMe highlighted that employees continue to be vulnerable to phishing attacks, with an average response rate of approximately 20% (Computer Fraud and Security, 2016; PhishMe, 2016). This includes responses to both spear phishing and generic phishing emails. This report, which was based on the analysis of over 8 million simulated phishing emails, also highlighted that 67% of employees who respond to simulated phishing attacks are repeat victims and therefore likely to respond to phishing emails more than once. The continuing vulnerability of many organisations to phishing attacks has led the UK National Cyber Security Centre to recently release specific guidance for organisations regarding how they can defend themselves from the phishing threat (NCSC, 2018a).

The hierarchical nature of many workplaces and employees' limited time means that they are likely to be particularly susceptible to the authority and urgency influence techniques highlighted by

* Corresponding author at: School of Experimental Psychology, University of Bristol, Priory Road, Bristol BS8 1TU, UK.
E-mail address: emma.williams@bristol.ac.uk (E.J. Williams).

https://doi.org/10.1016/j.ijhcs.2018.06.004
Received 23 June 2017; Received in revised form 23 April 2018; Accepted 30 June 2018
Available online 19 July 2018

Table 1
Example influence techniques that occur in phishing emails.

Technique	Description
Authority	Claims to come from an individual or institution that represents an authority figure.
Urgency	States that the receiver has a limited time to respond.
Reciprocity	Claims to provide some form of favour to the recipient.
Social proof	Suggests that other people have responded to the email.
Reward	Claims to provide the receiver with a potential reward if they respond.
Loss	Claims that the receiver will suffer some form of loss if they fail to respond.
Scarcity	Suggests that an offer or opportunity is limited in some way (e.g., for the first 10 respondents).

Cialdini (2007) and Stajano and Wilson (2011). Elements of the particular work context in which a spear phishing email is received (such as receiving an urgent request whilst being particularly busy or distracted) are also likely to exacerbate susceptibility. However, difficulties in accessing data related to susceptibility within workplace settings have severely limited current understanding of these factors. Therefore, there is much to be gained from investigating the role of both influence techniques and work-related contextual factors using applied data sources. This will not only aid theoretical development, but also assist in advancing practical interventions. The present paper uses data from two organisations that routinely handle sensitive information to address this current limitation; using a novel approach that enables existing theoretical concepts to be considered and new ones to be identified in relation to applied workplace settings.

The paper is structured as follows. First, we briefly consider current theoretical approaches and research findings relevant to susceptibility to spear phishing emails. We then present two studies conducted in organisational settings. In Study One, we take a novel approach to the examination of message-related factors (specifically, the presence of authority and urgency influence techniques) by examining historic data from simulated phishing tests within organisation A. In Study Two, we undertake a qualitative exploration of wider susceptibility factors related to the individual recipient and the context that they are in (including how familiar they are with the message sender, whether they are expecting a particular communication, and their awareness of the potential risk of spear phishing) by exploring employee perceptions of susceptibility within the work environment using a focus group methodology in a second organisation (organisation B). Although Williams et al. (2017a) discuss the potential role of these various aspects on susceptibility to online influence in their theoretical review, there is limited empirical evidence to date. The current studies take a first step in addressing this gap. We conclude by considering these findings in relation to the potential expansion of current theories. We also consider potential contributions to practical applications, including interface design, employee training and awareness, and decision support systems.

1.1. Theoretical justification

Over the last decade, researchers have attempted to identify the primary factors that may impact individual susceptibility to phishing emails. This has led to the development and application of a range of theoretical frameworks, including the Integrated Information Processing Model of Phishing Susceptibility (IIPM; Vishwanath et al., 2011), the Suspicion, Cognition, and Automaticity Model (SCAM; Vishwanath et al., 2016), and Protection Motivation Theory (PMT; Rogers, 1975). Although these models show a degree of overlap, they have rarely been studied together, despite the fact that all of the highlighted elements are likely to influence susceptibility to spear phishing. For instance, PMT has been more commonly applied to generic security behaviour and examines individual perceptions of threat and perceived ability to manage such threats. Conversely, the SCAM incorporates individual knowledge, beliefs and habits in relation to phishing susceptibility specifically. Finally, the IIPM focuses primarily on the information processing style that is used when a phishing email is encountered. These models have also not been extensively studied using organisational data. Exploring the role of all of these aspects within organisational settings provides a unique opportunity to understand the full range of factors that may influence susceptibility in the workplace. We further consider each of these models in relation to our study aims below.

1.1.1. The integrated information processing model of phishing susceptibility (IPPM)

The IPPM suggests that the likelihood that an individual will respond to a phishing email is influenced by the content of the email, such as the influence techniques that it contains, the use and accuracy of email signatures, and the sender address (Vishwanath et al., 2011). Specifically, the model claims that people's limited attentional resources are monopolised by the presence of particular influence techniques such as urgency (e.g., an urgent deadline). This increases the likelihood that people will rely on relatively automatic forms of information processing (known as *heuristic* processing) when deciding how to respond and will not engage in more in-depth consideration of the legitimacy of the email (known as *systematic* processing: Eagly and Chaiken, 1993; Harrison et al., 2016a; Kahneman, 2011; Luo et al., 2013; Vishwanath et al., 2011; 2016). As a result, authenticity cues within the email (i.e., features a person uses to determine legitimacy), such as an incorrect sender address, are more likely to be overlooked.

The relative role of particular influence techniques in influencing individual susceptibility to phishing remains uncertain, however (Oliveira et al., 2017). For instance, when comparing participant responses to genuine, phishing and spear phishing emails that contained authority, scarcity or social proof influence techniques, Butavicius et al. (2015) found greater susceptibility to emails that contained authority cues. Williams et al. (2017b) also manipulated the presence of authority cues within fraudulent software updates whilst keeping the presence of urgency cues constant and found that participants were particularly susceptible to updates containing authority cues. However, in a field experiment where different phishing messages were sent to more than 2,600 participants, the presence of authority influence techniques was not found to increase click-rates (Wright et al., 2014). In their analysis of participants' self-reported reasons for responding to fraudulent updates, Williams et al. (2017a) further highlighted the role of other message-related cues, such as how familiar participants were with the particular update message (i.e., whether they had received similar messages before) and whether they were expecting a particular communication.

To our knowledge, the relative role of such influence techniques has yet to be explicitly examined within workplace settings. This is despite the fact that particular influence techniques may be differentially relevant, and therefore have different effects, in work contexts. Within study one, therefore, we explicitly investigate whether the presence of authority and urgency techniques influence employee susceptibility to simulated spear phishing emails within the workplace. We extend this in Study Two by examining employee discussions of the message-related factors that they report as making them more or less likely to respond to an email that they receive.

1.1.2. The suspicion, cognition and automaticity model (SCAM)

The SCAM claims that the extent to which heuristic processing strategies are used when evaluating emails varies according to characteristics of the individual recipient (Vishwanath et al., 2016). These differences primarily relate to individual beliefs regarding online risk (Barnett and Breakwell, 2001; Bromiley and Curley, 1992), which encompasses the degree of experience, efficacy, and subject-specific knowledge that people have (Downs et al., 2006; Canfield et al., 2016;

Pattinson et al., 2012; Sun et al., 2016). However, the relationship between these factors remains unknown. A reliance on heuristic processing is considered more likely to occur when an individuals' ability or motivation to engage in more in-depth processing of information is reduced (Eagly and Chaiken, 1993). Therefore, individuals with a greater awareness of the risks of online activity, and phishing specifically, are considered more likely to engage in deeper processing of the information contained within emails, such as authenticity cues. Conversely, those with a lower awareness are considered more likely to engage in superficial, heuristic forms of processing. Finally, individual's established habits of behaviour in relation to email communications are also considered to influence the degree of suspicion that they have towards emails that they receive (Vishwanath, 2015; Vishwanath et al., 2016).

It is not clear, however, to what extent such constructs apply within a work context. For instance, people's beliefs regarding online risk may differ when they are at work compared to when they are at home, particularly if there are differences in how they may be impacted personally by any potential breach and the degree of IT support that they have available to them if they unintentionally respond to a phishing email., Similarly, the extent to which current training approaches provide sufficient knowledge to influence these beliefs and minimise employee susceptibility remains uncertain (Caputo et al., 2014). Finally, any potential relationship between these constructs and the information processing strategy that is used may be further influenced by wider aspects of the work environment, such as employees facing the additional challenge of being busy, distracted, or having other urgent primary goals competing for their time (Miarmi and DeBono, 2007; Sivaramakrishnan and Manchanda, 2003; Vohs et al., 2008).

Within Study Two, therefore, we explore the potential role of all of these factors within workplace settings. Specifically, we examine the extent to which these factors are reflected in employee perceptions of their own susceptibility to spear phishing. Such work is vital if the full range of potential interventions, including technical, training, process, and design solutions, are to be effectively exploited within organisations (Irvine and Anderson, 2006).

1.1.3. Protection motivation theory (PMT)

Protection motivation theory (Rogers, 1975) has been used to highlight the role of individual perceptions of online threats and perceived ability to cope with such threats in relation to security behaviour more generally (e.g., Ng et al., 2009; Tsai et al., 2016). PMT states that the likelihood of an individual engaging in protective behaviour is influenced by their perceptions of the particular threat (i.e., the perceived severity of the threat and their vulnerability to it) and the degree to which they feel able to enact the necessary behaviours to protect themselves (known as *self-efficacy*). PMT has recently been applied to the phishing domain. For example, a survey of 547 individuals conducted by Wang et al. (2017) demonstrated that people's 'phishing threat perceptions', combined with their (perceived) ability to detect phishing emails, impacted their resultant coping strategies. Namely, whether they focused on more effective, task-focused strategies, such as finding out more information and learning new skills to manage the threat, or more maladaptive, emotion-focused strategies, such as avoiding thinking about the issue. These coping strategies in turn influenced their ability to distinguish between legitimate and phishing emails. The potential influence of threat perceptions on responses to phishing emails was also discussed by Conway et al. (2017), who conducted a series of semi-structured interviews with employees regarding their experiences of information security and phishing. The findings of their analysis suggested that highly visible security procedures reduced perceived vulnerability to online threats in the workplace, resulting in less secure behaviour.

Within organisational settings, a number of technical and other support mechanisms may be in place to assist users on information security matters. For instance, the use of automated system alerts, specific phishing warnings circulated via email, and IT phishing-reporting mechanisms may all reduce perceived vulnerability and enhance self-efficacy in the workplace. However, there is very limited research exploring how people conceive of these mechanisms, the extent to which they may influence perceptions of vulnerability and self-efficacy, and whether employees consider them beneficial in helping them to effectively cope with the spear phishing risk. We explore the role of such factors in Study Two.

2. Study one

The primary aim of study one was to examine whether the presence of authority and urgency cues within simulated spear phishing emails differentially impacted employee susceptibility to these emails within a work context. Although phishing emails can make use of a range of influence techniques (Cialdini, 2007; Stajano and Wilson, 2011), the use of authority and urgency cues within phishing emails is known to be particularly commonplace (Akbar, 2014; Atkins and Huang, 2013). Authority cues focus on mimicking organisations or individuals that are respected and have a degree of authority in relation to the recipient. Urgency cues involve placing people under a degree of time pressure to encourage them to respond quickly. As previous work has shown that the presence of authority and urgency cues within phishing messages can increase susceptibility in other contexts (Butavicius et al., 2015; Williams et al., 2017a), we predict that these effects will extend to a workplace setting.

Hypothesis 1. The presence of urgency cues within simulated spear phishing emails will be related to an increased likelihood of responding to these emails.

Hypothesis 2. The presence of authority cues within simulated spear phishing emails will be related to an increased likelihood of responding to these emails.

2.1. Method

Historic phishing simulation data from a large UK public sector organisation (with >50,000 employees) that interfaces with members of the public and routinely handles sensitive information was analysed. This data was collected by the organisation and provided to the researchers in the form of aggregate responses to nine simulation emails that were sent to all employees of the organisation (approximately 62,000 individuals) over a 6-week period in early 2015. These simulation emails were sent from fictitious organisations and were specifically designed to closely mimic actual phishing emails that targeted the organisation. Each employee received two of these simulation emails.

A limitation of using these applied datasets was that we were unable to ensure that all simulation emails were sent to the same number of employees. Further, we did not have access to participants' demographic information. Table 2 shows the number of recipients for each of the nine emails. An example simulated phishing email is also shown in Fig. 1.

All emails were addressed to the individual recipient (e.g., 'Dear John') and contained a corresponding logo related to the fictitious organisation. As commonly found in phishing emails, each email also contained a link within the text that recipients were encouraged to click in order to respond to the email content. If recipients clicked on the link, they were automatically directed to an internal, educational website that informed them that they had clicked on a link within a phishing simulation and were provided with access to further voluntary online training and awareness-raising materials.

Each of the nine simulation emails were rated by two independent raters according to the degree to which the email included authority and urgency influence techniques. The content that was provided and assessed by the raters focused on information within the email body itself. This included the logo, the text of the email body, and the email

Table 2
General mean click-rate (CR) according to simulation email.

	Simulation email								
	1	2	3	4	5	6	7	8	9
Number sent	6,975	12,930	14,343	8,184	10,201	9,340	23,767	15,683	23,861
Number clicked	411	1089	4954	788	3303	2010	2190	5276	4737
CR	6%	8%	35%	10%	32%	21%	9%	34%	20%
Authority rating	R1: 1	R1: 1	**R1: 2**	R1: 1	**R1: 1**	R1: 1	R1: 1	**R1: 3**	**R1: 2**
	R2: 1	R2: 1	**R2: 2**	R2: 1	**R2: 2**	R2: 1	R2: 1	**R2: 3**	**R2: 1**
	MR: 1	*MR: 1*	***MR: 2***	*MR: 1*	***MR: 1.5***	*MR: 1*	*MR: 1*	***MR: 3***	***MR: 1.5***
Urgency rating	R1: 1	R1: 1	**R1: 2**	R1: 1	**R1: 2**	R1: 1	R1: 1	**R1: 1**	R1: 1
	R2: 1	R2: 1	**R2: 2**	R2: 1	**R2: 2**	R2: 1	R2: 1	**R2: 2**	R2: 1
	MR: 1	*MR: 1*	***MR: 2***	*MR: 1*	***MR: 2***	*MR: 1*	*MR: 1*	***MR: 1.5***	*MR: 1*

Note: R1 = Rating of rater 1; R2 = Rating of rater 2; MR = Mean Rating. Ratings in bold show emails included within 'technique present' group for each influence technique.

Fig. 1. An example simulated phishing email.

signature (as shown in Fig. 1). Raters were blind to the response rate (known as the 'click-rate') for each of the emails. Specifically, emails were rated on a scale of 1–3 (1 = not at all; 2 = slightly; 3 = very much) and raters were provided with standardised definitions to assist them:

- *To what extent does the email contain urgency-based influence techniques?*

Definition: The e-mail states that the receiver has a limited amount of time to respond if they wish to engage with the e-mail content, such as being time-limited, urgent or scarce. For example, 'this link will expire 24 h after this notification has been read by you.'

- *To what extent does the sender represent an authority figure or institution?*

Definition: The email contains cues that suggest that the sender has a degree of authority in relation to the recipient, such as the power to enforce compliance or give orders. For example, an email claiming to be from a senior figure within the organisation that requests individuals comply with a request.

Inter-rater reliability was assessed using Cohen's kappa (Dewey, 1983) and demonstrated good agreement between the two raters ($k = 0.745$, $p < .001$). For each phishing email, the score for each influence technique was calculated as the mean of the two raters' scores. These ratings are shown in Table 2.

In order to reduce the likelihood that any differences found between emails were related to other factors, such as the perceived authenticity of the email, all nine emails were also rated on the same 1–3 scale according to (a) the extent to which the layout of the e-mail appears genuine, (b) the extent to which the content of the e-mail appears genuine, and (c) the extent to which the email is considered to be trustworthy. For each of these aspects, all nine emails were rated > 1, with the majority > 2 (except email seven, which had a mean rating of 1.5 for layout, and emails five and six, which both had a mean rating of 1.5 for trustworthiness).

2.2. Results

Click-rate data was analysed according to the particular simulation email. Collapsed across email type, there was a mean click rate of 19.44% (*Range* = 6.00%–35.00%; *SD* = 11.85%), which reflects the average response rate of 20% highlighted in the recent PhishMe report (Computer Fraud and Security, 2016; PhishMe, 2016).

Due to a lack of data regarding which two emails employees received, each data point was treated as coming from a separate participant. For each of the four techniques, those emails that had a mean rating > 1 were labelled as 'technique present' and those that had a mean rating of 1 were labelled as 'technique not present'.

To examine the relationship between the presence of authority and urgency cues and mean click-rate, a binomial logistic regression was conducted in *R*, with authority and urgency technique (present vs. not present) as the predictor variables and response (link clicked vs. link not clicked) as the dependent variable.

The results demonstrated that both authority and urgency were associated with an increased likelihood of clicking on the email link (Authority: *Wald z-statistic* = 72.68, *df* = 1, $p < 0.001$, *OR* = 3.42, *CI* [3.31, 3.53]; Urgency: *Wald z-statistic* = 39.12, *df* = 1, $p < .001$, *OR* = 1.84, *CI* [1.79, 1.91]). This supports both hypothesis 1, that the presence of urgency cues will be related to an increased likelihood of responding to emails, and hypothesis 2, that the presence of authority cues will be related to an increased likelihood of responding to emails. For every one unit increase in authority rating, the log odds of clicking on the email link was found to increase by 1.23. For every one unit increase in urgency rating, the log odds of clicking on the email link was found to increase by 0.61. Finally, examining the difference between the residual deviance and null deviance allows performance of the model based on these predictor variables to be compared with a null model. The predictor variables were found to significantly reduce the residual deviance (*null deviance* = 122,136, *residual deviance* = 112,742, $p < .001$) compared to the null model, suggesting that they both contribute to model performance. These results are discussed in detail in Section 4: Discussion.

Email content is only one aspect likely to influence response behaviour, however. Since individual and situational-level factors could not be examined using the available phishing simulation data, further investigation was required to explore the potential contribution of these wider factors to employee response behaviour. Study Two was conducted to examine these factors, using a focus group methodology to explore employee perceptions of what influences their response behaviour.

3. Study two

The aim of study two is twofold. First, to examine whether factors external to the phishing message itself, such as aspects related to the individual recipient or the context in which they are operating, are likely to impact susceptibility to spear phishing within the workplace. Second, to examine whether specific factors identified in current theoretical models of phishing susceptibility (e.g., the IPPM: Vishwanath et al., 2011; the SCAM: Vishwanath et al., 2016; PMT: Rogers, 1975; further detail of specific factors is provided in Section 3.1.4: Thematic analysis) correspond with employee perceptions of their own susceptibility within the workplace. To address these aims, we employ a qualitative focus group methodology to explore employee perceptions of susceptibility to spear phishing emails. Specifically, six focus groups were conducted across two organisational sites of a second organisation (further details are provided in 3.1.3. Participants). These focused on examining employee perceptions of (a) the factors that impact susceptibility to spear phishing emails at work, (b) how they manage this susceptibility within the work environment, and (c) the perceived efficacy of current training approaches. In particular, the role of additional susceptibility factors external to the actual influence techniques used, such as habitual email behaviours related to work routines, phishing-related knowledge, and beliefs regarding phishing risk, was explored (Ng et al, 2009; Tsai et al., 2016; Vishwanath et al., 2016).

3.1. Method

3.1.1. Materials

A standardised question plan was developed to explore employee perceptions of their own susceptibility to spear phishing and how they manage suspicious emails at work. This enabled us to investigate responses in relation to current models of susceptibility to phishing (e.g., Rogers, 1975; Vishwanath et al., 2016; Vishwanath et al., 2016). This question plan was used as the basis for all focus groups and focused on the following areas:

1. What factors make you more or less suspicious of an email that you receive?
2. What factors make you more or less likely to respond to a targeted phishing email?
3. What factors make you more or less likely to report an email that you receive as potentially fraudulent?
4. What do you think about current training regarding phishing?
5. Anything else you would like to add regarding your interaction with targeted phishing emails?

Although the primary emphasis of the focus groups was on exploring susceptibility to targeted ‘spear phishing’ emails, focus group participants did make reference to generic phishing emails at various points. This was particularly prevalent when considering what made them trust an email. Where relevant, these points are highlighted in the results section.

3.1.2. Procedure

A qualitative approach was taken to enable perceptions and experiences to be captured and analysed according to the presence of theoretically-driven themes (for further details, see Section 3.1.4: Thematic analysis). This approach allowed us to take a more in-depth approach to exploring susceptibility factors, as well as identifying aspects of current training that could be improved. The study was granted ethical approval by the University's Research Ethics Committee (Ref. FBL.15.11.015). Focus groups were held on-site in a private meeting room. Two researchers were present at each focus group, with one facilitating the session and the second taking written notes. Each focus group was recorded using a Dictaphone and transcribed following the session. Any identifying information or reference to particular organisational systems was removed on transcription. Participants were provided with full details of the research prior to the focus groups and also provided informed written consent at the beginning of the focus group session. It was made clear prior to the focus group session that participation was voluntary and that participants could leave at any time without having to give a reason. Participants were also informed of general focus group etiquette prior to the start of the focus group. Thus, we informed participants that (a) we were interested in hearing their open and honest thoughts, (b) there were no right or wrong answers, (c) what is said in the room should not be discussed outside of it, and (d) that the session would be tape recorded, but individuals would remain anonymous in transcription and reports. Contact details of the researchers were also provided to enable participants to contact them in the future if required.

3.1.3. Participants

Thirty-two employees of an international organisation operating within the engineering and management sector (>10,000 total employees) participated in six focus groups conducted across two organisational sites within the UK in April 2016. Each focus group contained 4–6 participants. Participants were recruited via internal communications inviting employees to participate in a voluntary focus group conducted by university researchers to explore people's perceptions and experiences of targeted phishing emails within the workplace. Participants consisted of twelve males and twenty females and represented administrative, engineering and project management job roles. Further demographic information was not available to researchers.

3.1.4. Thematic analysis

Thematic analysis is a qualitative method that allows for interpretation of material to identify potential themes and patterns within the data (Berg, 2006). We adopted a hybrid approach, which included both inductive and deductive thematic analyses (Fereday and Muir-Cochrane, 2006). This involved three main stages: 1) inductive themes were defined according to the study objectives and in line with previous phishing susceptibility literature (e.g., the SCAM; Vishwanath et al., 2016), 2) subcategories (codes) within each theme were defined, and 3) emergent subcategories that were deduced from the data were defined. To illustrate, “4. Knowledge and Training” was predefined (and coded as a primary theme), and the corresponding categories were alphabetised, for instance, “4.a. Technical Understanding”. Emergent subcategories are highlighted with the corresponding codes, for instance “4.b. understanding the security centre (emergent)”. The thematic framework is outlined as follows:

1. **Trust or suspicion**
   Definition: Concepts and perceptions related to factors that make someone consider that an email is likely to be legitimate or that make them doubt its authenticity. Based primarily on research of Vishwanath et al. (2011; 2016) and Williams et al. (2017b).
   Codes: (a) Determining authenticity; (b) familiarity; (c) expectations; (d) work context.
2. **Perceptions of spear phishing risk**
   Definition: Concepts and perceptions related to people's perceived vulnerability to spear phishing within the work context, and the perceived severity if this occurred. Based primarily on Protection Motivation Theory concepts (e.g., Rogers, 1975; Tsai et al., 2016).
   Codes: (a) Exposure to external emails (emergent); (b) centralised inboxes (emergent); (c) risk awareness.
3. **How susceptibility is managed**
   Definition: Factors related to the mechanisms that people use to help them manage spear phishing emails in the workplace. Based primarily on discussions with organisational security personnel.
   Codes: (a) Warnings and banners; (b) reporting; (c) peer verification

(emergent); (d) avoidance (emergent).

4. **Knowledge and training**
   Definition: Factors related to the degree of knowledge that people have regarding spear phishing emails. Based primarily on research of Vishwanath et al. (2016) and discussion with organisational security personnel.
   Codes: (a) Technical understanding; (b) understanding the security centre (emergent); (c) information overload (emergent); (d) perceptions of training.

Two independent coders who were both present in the focus groups analysed the dataset. Inter-rater reliability was assessed using Cohen's kappa and demonstrated good agreement between the two raters ($k = 0.890$, $p < .001$). There were 21 instances where the two coders coded the same information differently. These discrepancies were resolved through discussion between the coders and a third individual who was not present in the focus groups but had knowledge of the research area.

3.2. Results

3.2.1. Theme 1: trust or suspicion

In all of the focus groups, the majority of participants had received some form of phishing email, although these were often related to a personal context rather than the work environment. These experiences often reflected more generic phishing scams, whereby the content of the email and sender address were highlighted as containing a number of 'suspicious' cues that were generally easy to identify, such as receiving emails that claimed to be from a legitimate organisation but that came from a personal email address: *"at home you get ones like 'inland revenue at google.com'." (FG6, P1)*. The majority of factors that were identified as impacting trust of an email were applicable to both a home and work context, with only some specific aspects reflecting the particular work environment. These factors are discussed in more detail below.

(a) Determining authenticity

Particular aspects of an email that are used to determine authenticity were highlighted a total of 32 times across all six of the focus groups, focusing primarily on actions such as hovering over the hyperlink and examining the sender address for errors, thus demonstrating a degree of knowledge and awareness of how to identify fraudulent emails. For example, *"the easiest way I find is to click on the email address it comes from" (FG1, P2)*. Similarly, the presence of spelling errors was consistently highlighted as a suspicious cue, *"I had one from Barclays before, it had the Barclays logo and everything and I think on the first or second paragraph they spelt Barclays wrong, so…" (FG6, P2)*. In addition to these more specific elements, subjective judgments of something feeling 'not quite right' were also considered, particularly when other aspects of the email appeared legitimate. For example, *"something I always just can't figure out, you know, human nature, is when they look fine, almost too perfect, and there's something about them, but it doesn't look like spam at all, it's just a lovely, perfectly worded email, brilliantly laid out and then you catch a feeling and think 'why am I even thinking about this?', most emails you don't even question, but you get that feel, bad vibe from it" (FG6, P2)*. A greater requirement to base decisions on these subjective feelings was explicitly highlighted in roles where more traditional cues, such as sender address, could not be relied upon. For example, *"I suppose that is it though, where they've come from. I mean I work in procurement and you get legitimate enquiries wanting to be a supplier and all that and it's often necessary to open the email to check that, that sort of content, you can't just go by the address that it's come from necessarily… but they've usually got something not quite right in them, haven't they, which rings alarm bells" (FG5, P5)*. The majority of these elements were considered relevant to both spear phishing and generic phishing emails, although the topic of the email was considered most relevant for generic phishing (e.g., whether it represented a typical '419' scam offering vast sums of money).

(b) Familiarity

Relative familiarity with the sender or topic of emails that are received was mentioned 10 times across five of the focus groups. For instance, being unfamiliar with the sender of the message was considered an important cue by some participants, *"I suppose I'm a bit paranoid, if I don't know the person who sent it to me, even if it looks genuine, if there's an attachment then I don't open it" (FG2, P2)*, although this was more qualified in others, *"if it's an unknown sender, I might be suspicious" (FG5, P2)*. New employees who were not yet familiar with the individuals that they would typically be liaising with were also highlighted as potentially being more susceptible to phishing emails, particularly those emails that established members of staff would consider relatively easy to identify. For example, *"when I first came here, I was, because I wasn't familiar with what the companies were that were going to email me necessarily I was just sort of clicking on anything … but it was just because I wasn't familiar with the companies that we were dealing with" (FG4, P2)*. Despite the use of familiarity as a potential cue to the legitimacy of an email, the potential risks of familiar senders were also highlighted by one participant, "*they can be the hardest ones to spot sometimes, if they're from a friend or contact and they've actually been hacked haven't they and sometimes they can be the tricky ones to work out" (FG1, P2)*.

(c) Expectations

Communications that were expected or considered routine were also highlighted as less likely to trigger suspicion, being mentioned 26 times across all six focus groups. For instance, one participant discussed receiving an email at *"two minutes to midnight on a Saturday and we just thought, you know, so we just sent it straight to [IT Security] here at the time and said, you know, we never, no one would ever send us an email at that time in the morning with this sort of heading on it" (FG2, P3)*.

However, the presence of expectations regarding communication norms and what a legitimate message typically 'looks like' could also lead to issues in itself. For instance, difficulty in identifying fraudulent emails that exploit these expectations and routines was explicitly highlighted by one participant in relation to a colleague who had received a spear phishing email regarding an unpaid invoice from a legitimate email account: *"it's a company she deals with, we've currently got problems with accounts payable … and actually why would she not believe that it was true" (FG1, P4)*. Particular expectations regarding communication norms were also highlighted as leading to difficulties in international working environments. For instance, different email styles and communication norms across different countries could make it more difficult to differentiate legitimate emails from spear phishing emails: "*I mean there are some places, you do get, you get some emails from America and they write in a different way and it does make it difficult sometimes to sort of spot the difference" (FG6, P5)*.

(d) The work context

The role of the work context in influencing responses was highlighted 13 times across all of the six focus groups. The impact of being busy on the depth of information processing that was possible was highlighted in the comments of one participant, *"I think that you're still likely to click on something because we're all really busy and I think that you sort of scan stuff don't you, and if you see something attached you might just click and think 'oh well, I'll have a look at the other information', you don't always have lots of time" (FG1, P4)*. Similarly, another participant stated *"Yes, if it was out of my sphere of what I was doing, say I was doing, I don't know [project related task] and I got an e-mail about something else I'd think, 'why do they want to know that?' but again if you're very, very busy*

then I might just click on it by accident" (FG2, P1). This issue was also highlighted by one participant as being particularly relevant in smaller businesses, who may not have the IT support and reporting infrastructure to allow people to easily verify the legitimacy of emails if they do have concerns, *"everyone's way too busy, so you know 'I haven't got time to check that' so, I don't know, they [larger businesses] may have people who it might be their entire job to check these emails which is great, but then, for other people, a smaller business, where they don't have that, they don't have that kind of support" (FG6, P2)*.

3.2.2. Theme 2: perceptions of spear phishing risk

The extent to which participants were exposed to spear phishing emails within the work context varied substantially, with some participants reporting that, (to their knowledge) they had never received a phishing email of any kind whilst at work, whilst others reported receiving targeted emails on a regular basis. This exposure appeared to be impacted by the extent to which individuals received external emails within their job role and the use of centralised inboxes. Those with greater exposure to spear phishing also demonstrated a greater degree of awareness regarding how to report phishing emails, as well as the risk of being targeted by spear phishing emails within the workplace. These factors are discussed in more detail below.

(a) Exposure to external emails

Exposure to external emails was discussed eight times across five of the focus groups. If individuals did not regularly receive external emails, then receiving such an email was highlighted as a primary trigger for suspicion in the work context:

"*P3: we shouldn't also get ones from outside influences*
P2: no
P3: the external ones, for example, we shouldn't get on a day to day basis, it should be from [internal] personnel and that would flag it up for me…
P1: yeah, [internal] are the only ones we should be getting, unless you're doing a task outside
P3: yeah".
(FG2)

For employees who regularly received external emails, it was considered more difficult to determine the authenticity of an email. As stated by one participant, *"ours will be from everywhere, because we buy an awful lot of stuff from outside companies, [organisation] and what have you, I've noticed more and more emails are coming through which I just put as junk, junk, junk, but yeah and we have so much coming through that it could be easy to click on something" (FG2, P4)*. Such difficulties were also highlighted by a call-centre based employee, *"we get 200–300 emails a day, so knowing when to click on something and when not to click on something is quite hard because we get purchase orders coming through and we've got to click on the attachment" (FG5, P1)*.

The substantial variation in exposure to spear phishing across job roles was reflected in employees' relative awareness of the relevant processes and procedures, such as how to report a suspected phishing email, with those who regularly encountered potentially fraudulent emails or regularly reported emails as suspicious appearing to be more familiar with the reporting process. As highlighted by one participant who did not regularly encounter 'suspicious' emails, *"to be honest I wouldn't know, I don't generally get phishing emails at work and I wouldn't know who to report it to, the IT department I guess" (FG1, P2)*.

(b) Centralised inboxes

Job roles that involved use of a centralised inbox were also highlighted in two of the focus groups as increasing exposure to potential phishing emails: "*we get them, sort of, every day because we have several centralised inboxes, so we'll get a phishing email every single day" (FG5, P1)*. Similarly, *"I mean I haven't had it here, but when I worked in a different building we had our co-owned little email address, I used to get quite a few, you know, sort of unsolicited ones and I thought, always forwarded them on and they came back to me and said no it was ok but thank you…" (FG1, P5)*. These emails could include both generic phishing and targeted phishing emails. For the latter, other cues that would traditionally raise suspicion, such as an unexpected contact, were also deemed to be lacking due to the unsolicited nature of some messages, thereby increasing the reliance on external verification and reporting procedures. For instance, *"its very difficult for us because I think our inbox allows every single thing you could imagine come through, whereas, personal [personal inbox], I've only ever had one come through on that, but our centralised one we have to allow anyone to pop an email in that so it gets quite difficult" (FG5, P1)*.

(c) Risk awareness

Differences in perceptions and awareness of risk were referenced 16 times across four of the focus groups. This was explicitly highlighted by one focus group participant, *"I don't think it's something that is well understood … I think it's mixed, you've got people who are very clear about it and you've got people who aren't so clear… or aren't so clear on what their regular routines and habits and ways of dealing with emails might cause… I think that there's a spectrum of awareness around it" (FG3, P1)*.

Differences were also highlighted according to perceptions of risk and vulnerability within a personal (i.e., home) context compared to a work context. In particular, the work environment was perceived as more secure, with enhanced technical controls making it less likely that suspicious emails would be encountered (although this was dependent on the job role), and the provision of specialist support to reduce the impact if a phishing email was responded to. For instance, one participant questioned *"are we distinguishing between work and home perhaps, because I think at work it's not so prevalent because this should be a better system in place for it hopefully" (FG5, P2),* whilst another highlighted *"that's a good thing about work though, as it's a good system so a lot of them get blocked, so we don't generally get much spam or kind of stuff through the work email address, with my [personal] account I get a big problem with that" (FG1, P1)*. In contrast, perceptions of vulnerability in a personal context appeared to vary substantially, with some participants demonstrating a high degree of confidence in their ability to manage phishing emails of all types and others feeling much more vulnerable. For example, *"see I feel quite comfortable with them at work, they'll let me know not to open it, at home… you just don't know what to do" (FG4, P4)*.

3.2.3. Theme 3: how susceptibility is managed

When discussing the potential risk from spear phishing within the workplace, employees highlighted a number of assistance mechanisms and aides that they used to manage this risk in their day-to-day environment. This ranged from online warnings and email banners to reporting mechanisms and discussion with peers.

(a) Warnings and banners

The perceived benefit of technical-based aids for focusing attention and invoking suspicion were highlighted nine times across all six focus group, with particular reference to the use of email banners to encourage users to engage in more systematic consideration of the email. For example, *"now they have an external email banner, which helps because it does make you think to look at it more and don't click on anything" (FG2, P4)*. The provision of security alerts was also considered to increase awareness of particular threats, providing a means to match emails received with a mental representation of a known phishing threat and making it less likely that such emails would be considered genuine.

"P4: they tend to send like an alert saying if you get something from this

specific address or saying this, some people have been targeted … which is quite useful, so you can at least see the body of the text and go 'ah yeah, if I see something like that'…
P3: yeah, that's a good thing
P2: yeah, that's all I generally see, are alerts saying watch out for this". (FG1)

(b) Reporting

The use of reporting procedures to determine the legitimacy of emails was discussed 40 times across all six focus groups. The ease of reporting potential phishing emails, and the provision of timely and reliable feedback in relation to the legitimacy of these emails, was highlighted as helping employees make the correct decision regarding emails that they were uncertain about. For instance, *"there's a spam reporting email that they've got set up, you just attach it to that, send it off, wait for it to come back telling you whether it is or not" (FG2, P4)* and *"yeah, we just send them off to another email address and then it comes back to us saying it wasn't malicious or whatever" (FG5, P1)*. Receiving consistent and timely feedback was seen as vital to make sure that people did not consider their reporting actions a waste of time and thus be less likely to report emails in the future, *"yeah, if you're not getting any feedback at all then you'll stop forwarding them on, make you think 'are they paying any attention?" (FG1, P2)* and *"I guess I might be more resistant to send it off if I think it takes two days to get back and for them to say 'oh you can open it' and then I'm two days behind in my work" (FG6, P2)*. A number of participants also highlighted other factors that may reduce the likelihood of reporting, such as a fear of potential negative repercussions, *"I just know people who haven't wanted to report things because they thought they would get into trouble for clicking on something" (FG2, P2)*, not considering it important, *"if I see something I'm not expecting to get I'd probably just delete it without opening it up. I don't think I'd report it to anyone" (FG5, P3)*, and the potential time involved, *"the first time I got one I thought, in the back of my mind, there was a 'we're meant to report all spam, aren't we' but I had to go on [intranet] and Google, well, search, for how to do it. It's not the easiest thing to find on [intranet], if it's something that happens so rarely you're not going to remember" (FG6, P3)*.

(c) Peer verification

The role of peer support in verifying emails, such as speaking to colleagues, sharing tips or getting advice from others with regards to decision-making in conditions of uncertainty, was also discussed 11 times across five of the focus groups. In particular, the extent that other members of staff also received a particular email appears to influence decision-making.

"P3: so when you pass it around, you say 'have you seen that email' and you say 'yeah, what did you do with it?', 'delete it', 'I'm sending it on', you know that comes round in the office quite often, you know in an office with [x] people sitting around and all of a sudden you all get this email and you think it must be phishing if we've all got it.
P6: but then, if it was just you then you might be less sure, you know 'have you got this?' 'no', it might be phishing, but it might not, so you'd still be on your guard but less so I guess, I don't know".
(FG2)

This social verification was considered particularly relevant for new staff, who may be uncertain regarding communication norms within their job role, and for those who did not regularly receive suspicious emails. For instance, one participant recounted receiving a particular email in the office, *"I was like, hey [name], I've got an email, this is exciting it's from [name department] and he was like, 'don't click it' and I was like 'oh, sorry" (FG6, P4)*. Similarly, another participant recounted a similar incident, "*I said to my colleague, 'oh, I don't really understand', and she said, 'oh my god, don't open it, don't open any attachments, send it on to the spam', so I was like 'oops, thank you" (FG4, P2)*. However, staff groups who do not have access to such informal support mechanisms, such as remote workers or those working off-site when an email is received, may be at particular risk in this regard.

(d) Avoidance

Avoiding engaging in activities that may increase the risk of falling victim to a phishing attack, such as refusing to click on links within any email received, was also highlighted as a means of reducing susceptibility across three of the focus groups. However, this strategy could only be used if the email or link was not perceived as necessary for work activities. For example, *"I don't click on anything if I can help it. I don't click on anything, even if it looks legitimate, unless I feel I need to do that for my work… how do you know, I mean, how do you know it's safe?" (FG3, P6)*. In scenarios of goal conflict, therefore, where an email is considered important or necessary for a work task, such strategies may prove difficult to enact.

3.2.4. Theme 4: knowledge and training

Finally, a number of factors were highlighted regarding the degree of knowledge that employees have about both spear phishing and phishing in general, including how and why user information may be gained and used, how security systems manage the phishing risk, and the perceived effectiveness of training in this area.

(a) Technical understanding

A number of issues were raised in focus group discussions that reflected uncertainty regarding what spear phishing encompasses, how personal information may be gathered and used in spear phishing attacks, and potential trajectories of impact within a system if such an email is responded to (i.e., once a link has been clicked or user credentials entered). Overall, this was referenced 12 times over five focus groups. For instance, *"regards to everybody in the company, what, if you asked the question to someone in the company, what is phishing, … they'd say 'I know its something to do with emails', but what is, you know, what is spam, 'well, they're all the same aren't they?' well, they're not, you know, so maybe we need to tell people exactly what each thing is and the key things to looking out for them" (FG2, P3)* and *"So, I don't think that people actually know what happens if you do accidentally click on something" (FG3, P4)*. Aiding individuals to gain greater understanding of both the consequences of their potential actions and how these consequences can be mitigated at each stage was considered important, *"I think it might be worth when they're doing the training taking a hypothetical scenario saying right Miss A is sitting at her desk and she clicks on this, this is what it's opening up, this is here it's going to, this is what it's leading to, this could be the consequences, so you can see how one click… could almost bring down a company. I don't think people realise just how consequential it can be" (FG4, P4)*.

(b) Understanding the security centre

Uncertainty regarding technical security systems, including how these work and how they are operated, was highlighted seven times across four of the focus groups. For instance, uncertainty regarding the vulnerabilities of technical systems was highlighted by one participant: *"I think I have an expectation now that we're a [particular type of company] our IT department should be able to deal with most sort of, attempted attacks on our systems, so I sit there thinking well I don't need to worry about it too much … for me, they should be the ones maybe where the investment is to try and stop as many as they can, because by the time they get to us it's kind of failed all of the different sort of checks that must be in place" (FG1, P4)*. Uncertainty regarding the degree to which processes can be, and are, automated was also considered. For instance, *"what I don't know is what the process is for, once you've reported it, is there a physical person that has*

to check it, or is there some sort of automated system, because depending on, if I was reporting sort of one a day I think I might feel I'm overloading this poor person with all these emails" (FG6, P3).

(c) Information overload

In order to enhance and maintain employee awareness of spear phishing attacks, communication materials may be regularly circulated to employees via a range of mechanisms (e.g., posters in corridors, information on noticeboards, intranet articles etc.). However, when combined with the vast array of other information that must also be routinely circulated to employees, such as health and safety information and site-specific news, this was considered easy to miss or forget. The issue of an overload of protective information of various sorts was highlighted five times across five of the focus groups.

"P4: we do get bombarded with quite a lot of different things about security and health and safety

P5: see that's the thing, which all come through on email so it's clogging up your email, making it worse, so you just randomly go through thinking 'that'll do'

P4: and also on the noticeboards, I think we're probably a bit blind to it …

P2: I think that in our specific area we do get a lot of security things so, yeah, some of it might get missed or forgotten".

(FG1)

(d) Perceptions of training

The efficacy of current training was considered 26 times across the six focus groups. When considering current training, the majority of participants perceived this in relation to a 'tick-box' exercise, with individuals completing online modules either when they are short on time or overloaded by information from other courses (e.g., during the induction period). This was considered to result in the information 'not going in', suggesting that training content is not sufficiently processed to ensure that it can be easily recalled when required.

P1: they [people] just want to get their pass and then forget everything about it, that's the main thing

P3: yeah

P5: most people just go to the assessment at the end and never actually… and don't bother actually reading it all".

(FG1)

Current training approaches were generally considered to be too static and unresponsive to the changing cyber domain. For instance, *"the variation is not that great, you know everybody's saying on the news and everything else, this is getting worse and worse and worse, but the questions are the same as we had last year" (FG2, P1)*. Overall, participants highlighted a number of suggestions for improving current training approaches in order to more effectively address perceived susceptibility factors. These included:

- Providing greater detail
- Regularly updating content
- Allocating specific time to complete training outside of the primary job role
- Using a range of interactive methods (particularly discussion-based activities)
- Ensuring personal relevance.

Potential implications of these suggestions for practitioners are discussed within Section 4.2: Implications for Designers and User Communities.

4. Discussion

These studies explored the factors that influence susceptibility to spear phishing emails within the workplace. Study One used historic phishing simulation data to examine the impact of message factors, specifically the presence of authority and urgency influence techniques within the email, on susceptibility to phishing within an ecologically valid context. In line with our hypotheses, significantly higher click-rates were found for phishing simulations that contained authority and urgency cues. Study Two was then conducted to examine the potential role of factors external to the message itself on employee susceptibility, with a particular focus on perceptions of spear phishing risk, degree of knowledge, work-related routines and norms. This allowed the influence of context, specifically that of the work environment, to be explored in a novel and practically relevant way. Applying concepts from theoretical models to data collected in an organisational setting not only provides a degree of validation within applied contexts, but also aids theoretical development through the identification of additional concepts of interest. Overall, the primary factors highlighted in current theoretical models of phishing susceptibility were supported. A number of additional factors specific to work contexts were also identified, including degree of exposure to external emails, the use of centralised inboxes, information overload within the work environment, and the role of social and technical support in enhancing perceptions of self-efficacy. This provides a basis for the further development of current theoretical approaches (Ng et al, 2009; Tsai et al., 2016; Vishwanath et al., 2011; Vishwanath et al., 2016), as well as a number of practical recommendations relating to interface design, employee training and awareness, and decision support systems. These are discussed in more detail below.

4.1. Theoretical implications

4.1.1. Understanding message-related factors: the IPPM

When considering what makes people susceptible to phishing emails, the IPPM claims that influence techniques contained within such emails (such as an urgent deadline) distract people's limited attentional resources away from important authenticity information (such as the accuracy of the sender address; Vishwanath et al., 2011). Within the reported research, we found that the presence of common influence techniques within spear phishing emails (specifically, urgency and authority cues) contribute to increased susceptibility within a workplace setting, likely by encouraging the use of heuristic processing strategies (Vishwanath et al., 2011). Since the IPPM was primarily developed and tested within a university population, these findings provide novel evidence that such concepts also apply within a workplace domain where employees have previously received a base level of cyber security training.

Interestingly, when participants within Study Two considered the factors that they believe influence their email response behaviour, the specific influence techniques highlighted in study one (i.e., authority and urgency) were not mentioned. Instead, participants focused predominantly on whether they were familiar with the message sender, whether they were expecting the communication, and the presence of authenticity information, such as a correct sender address. To a degree, this is unsurprising since it has previously been acknowledged that familiar information is more likely to be considered legitimate due to increased accessibility of that information within memory processes (Begg et al., 1992; Polage, 2012). However, although it is possible that participants implicitly considered aspects related to authority influence techniques when discussing authenticity information, this was not stated and does not consider other influence techniques, such as urgency. This suggests that individuals may be unaware of their vulnerability to the influence techniques commonly contained within spear phishing emails, representing a gap in current knowledge. As a result, although employees identified authenticity cues as a means to identify

spear phishing emails, these strategies may fail if the email contains well-crafted influence techniques or if they are operating within a pressured cognitive context at the time that the message is received (Williams et al., 2017a). This is in line with the heuristic processing propositions of the IPPM and the findings of study one.

Within current models, the degree of correspondence between what an individual perceives to influence their judgements (i.e., sender address etc.) and what is actually found to influence them (i.e., the presence of authority or urgency cues) is not currently specified. The findings of our study suggest that there is currently a dissonance between these two aspects. Susceptibility to influence techniques may thus be driven by either a lack of understanding regarding how such cues can be used within spear phishing emails or a lack of understanding of our own vulnerability to such cues. Future work should directly address these possibilities. In particular, whether greater knowledge of influence techniques reduces their persuasive effect or whether such techniques are capable of encouraging heuristic processing irrespective of the degree of awareness that an individual has.

4.1.2. Risk beliefs, knowledge and habits: the SCAM

The SCAM proposes that the beliefs that an individual has regarding online risk and their established habits of behaviour influence the information processing style that is employed when an email is encountered (Vishwanath et al., 2016). Within study two, work-related norms and routines, online risk beliefs, and degree of knowledge, were all explicitly highlighted by employees as likely to influence their susceptibility to spear phishing.

A number of examples of spear phishing emails exploiting habits and routines were identified. These were likely to encourage a reliance on heuristic processing strategies, effectively slipping under the radar and leading to individuals clicking automatically whilst engaged in their usual job routine. For example, an email matching prior expectations was considered to increase the likelihood that a quick 'scanning' of email content would occur. Emails were also identified that mimicked familiar senders or 'usual' subjects, making it less likely that they would 'stand out' from other communications that are received (Grill-Spector et al., 2006; Taylor and Fiske, 1978). Unless an email is perceived to be abnormal in some way, it is unlikely to trigger more in-depth, systematic processing and the additional time and mental resource that this involves (Vishwanath et al., 2016). Although some people reported being generally more suspicious of emails than others (in line with findings of Harrison et al., 2016b), suspicion was also often triggered by particular norms related to the individual's job role. For instance, employees who did not routinely receive external emails highlighted this as a 'red flag', whereas those who regularly received legitimate external emails had to use other triggers to guide decision making, such as whether the email countered expectations. These decision processes appear to be primarily related to differences in the degree of exposure to phishing emails within the work context, with employees who more regularly receive spear phishing emails highlighting the use of more considered processing strategies in order to counter the perceived risk. Finally, work-related pressures that were considered a routine part of the work environment, such as being interrupted during a work task (Hodgetts and Jones, 2006), being otherwise distracted or in a rush (INFOSEC Institute, 2013; Miarmi and DeBono, 2007), or being cognitively fatigued in some way (Vohs et al., 2008), were also considered to increase susceptibility.

Although some of these aspects are accounted for by the role of email habits and experience highlighted by Vishwanath et al. (2016), our findings suggest that a wider consideration of 'norms and routines' should be included within theoretical models that explicitly accounts for (a) the degree of familiarity with communication types, (b) prior expectations regarding specific communications, and (c) context-induced cognitive pressure within the work environment. For instance, cognitive pressure is likely to increase reliance on heuristic processing and therefore should increase susceptibility. Conversely, particular communication expectations within a job role could result both in decreased susceptibility to phishing emails that counter these expectations, and increased susceptibility to spear phishing emails that exploit these expectations. Systematic investigation of the relative influence of these various factors on response behaviour and how they may interact across different contexts is required.

Finally, the SCAM claims that increased knowledge and experience regarding phishing will contribute to more accurate cyber risk beliefs, thus reducing the likelihood that individuals will rely on heuristic processing strategies. Spear phishing emails represent a particularly difficult to spot attack, and if individuals do not have relevant experience of targeted phishing emails (whether through direct experience or education / training), they may be particularly vulnerable to emails that do not match 'typical phishing' stereotypes. This was evident in the wide range of phishing knowledge demonstrated across participants, with some demonstrating a high degree of understanding regarding how various forms of information can be used to design a spear phishing attack and others unfamiliar with potential spear phishing risks. Again, participants with greater exposure to spear phishing emails within the workplace appeared to demonstrate greater knowledge and more accurate understanding of phishing risks. When assessing the risk of becoming the victim of a spear phishing email, individuals are likely to make judgements about their vulnerability based on previous experience and information regarding the experiences of those around them (Barnett and Breakwell, 2001). As such, those who do not generally encounter phishing emails of any kind within their job role may consider themselves less vulnerable to phishing more generally. Unfortunately, this may make them less likely to consider the possibility that an email may be fraudulent if they are ever actually targeted. However, it is also possible that those who regularly receive particular types of spear phishing emails may indeed be more adept at identifying suspicious emails that match these expectations, but may be more susceptible to those that do not. Our findings suggest that these relative differences in exposure, and their resultant impact on phishing-related knowledge, risk perceptions, and context-specific suspicion should be further investigated and accounted for in current theoretical models (Rogers, 1975; Vishwanath et al., 2016).

4.1.3. Coping with spear phishing in the workplace: PMT

PMT (Rogers, 1975) posits that individuals will engage in a particular protective behaviour if they feel that the threat is sufficient and they feel able to enact the protective action (*self-efficacy*). Within Study Two, a number of technical and other support mechanisms and aides were identified by participants as reducing perceived risk in their day-to-day environment and helping them to cope with spear phishing in the workplace. These included technical-based aids (warnings and banners), IT reporting mechanisms, and peer verification. Interestingly, these reflected the predominant susceptibility factors highlighted by current theoretical models (Ng et al., 2009; Tsai et al., 2016; Vishwanath et al., 2011, 2016). For instance, technical design solutions often direct an individual's attention to elements of the message that may raise suspicion, such as online warnings and external email banners (Modic and Anderson, 2014). Such approaches have the potential to override greater attentional focus on the influence techniques contained within the message content. Similarly, mechanisms of verifying initial suspicions via expert feedback or discussion with peers provide feedback regarding current risks in the workplace (Woolley et al., 2010). This may be particularly beneficial for users who lack in-depth knowledge and may not feel sufficiently confident to risk not responding to an email in case it is legitimate. The presence of influence techniques that invoke compliance with authority or urgency cues may exacerbate this further, whereby signalling distrust of the email could be perceived as carrying a potential cost with regards to the message sender or scenario (ten Brinke, Vohs and Carney, 2016).

Overall, the range of assistance mechanisms highlighted within Study Two portray the range of ways in which employees attempt to

manage perceived vulnerability to spear phishing at work. These findings also extend the PMT concept of self-efficacy within the online security domain by identifying particular mechanisms through which self-efficacy may be enhanced (i.e., online warnings and banners, expert feedback, peer verification). For instance, email warnings and banners may increase perceived ability to identify a spear phishing email by assisting people to identify suspicious elements of a communication (e.g., an external sender) and match incoming emails with known phishing attacks. Conversely, expert feedback and peer verification provide support for those who are not confident in their ability to detect a spear phishing attack by providing a means to independently verify any doubts or suspicions that they may have.

Finally, a small number of employees also highlighted avoiding clicking on any links within emails as a risk-reduction strategy. However, this strategy could only be used if the email or link was not perceived as necessary for work activities, highlighting the precarious balance between operational and security requirements within the work environment (Kainda et al., 2010). In scenarios of goal conflict, where an email is considered as potentially important or necessary for a work task, such strategies may prove difficult to enact. This may lead to final response decisions being dependent on the particular organisational security culture within which the employee is operating (Rocha-Flores and Ekstedt, 2016), their perception of the relative risks of clicking on a particular link (Ng et al, 2009; Tsai et al., 2016; Vishwanath et al., 2016), and the extent to which the email reflects current work-related demands and pressures. As a result, such avoidance strategies may actually represent a maladaptive form of coping that is enacted when perceived self-efficacy to effectively identify a spear phishing email is low and alternative verification strategies are not considered effective or timely. Our findings suggest that the potential influence of work context, and the assistance mechanisms that it does (or does not) provide, on perceived self-efficacy should be further investigated. In particular, survey approaches that assess self-efficacy both before and after exposure to particular assistance mechanisms, and its relationship with actual detection ability, would be beneficial.

4.2. Implications for designers and user communities

There is continuing debate regarding the utility of phishing simulations within organisational contexts, with suggestions that such approaches fail to address the complexity of phishing vulnerability and contribute to the development of negative, blame-based security cultures (National Cyber Security Centre, 2018b). The findings of this paper highlight the complex nature of susceptibility to phishing within the workplace. If effective mitigations are to be developed, it is necessary to first understand the underlying causes and mechanisms driving response behaviour. It is increasingly clear that a one-size-fits-all approach is unlikely to be sufficient, with the wider message, individual and context-related factors identified in this paper requiring attention. For instance, employees were found to display large variation in their exposure to spear phishing emails within the work environment, primarily driven by the extent to which they received external emails, with staff groups who regularly deal with external suppliers having the most experience of both receiving and reporting spear phishing and generic phishing emails. Whereas this increased exposure could lead to increased susceptibility in such groups, it could also result in enhanced awareness of the risks of spear phishing and how to deal with it, due to the regular requirement to make decisions regarding message legitimacy.

Responding to these different exposure patterns may require the development of adaptive user interfaces that respond to the likely awareness of users, with those who are less regularly exposed to phishing emails requiring different system sign-posting. For instance, less aware users may respond favourably to periodic reminders of the phishing threat and how to report phishing emails. Conversely, more aware users may benefit from regular updates regarding evolving phishing tactics in order to counter any potential stereotypes that may develop through repeated exposure to similar targeted phishing emails (e.g., invoice scams). In order to achieve this, an in-depth analysis of the potential impact of particular job roles on phishing susceptibility using existing human factors tools, such as task analysis (Kirwan and Ainsworth, 1992) may be of benefit in identifying and mitigating likely risk factors for different staff groups.

To enhance and maintain employee awareness of phishing attacks, communication materials are often circulated to employees via a range of mechanisms (e.g., posters in corridors, information on noticeboards, intranet articles etc.). However, it is well established that an individual's attentional resources are limited (see Kahneman, 1973), with restrictions on the amount of information that cognitive systems can process at any one time. When these materials are combined with the vast array of other information that must also be routinely circulated to employees, such as health and safety information and site-specific news, this can reduce the likelihood and extent that such information will (a) be noticed, and (b) be remembered or applied when making decisions regarding the legitimacy of emails. This issue is also likely to be accentuated by other aspects of the work environment, such as a perceived lack of time to undertake tasks outside of the primary job role, which can lead to additional information not being prioritised. The allocation of specific time to interact with such information, or the use of more creative, interactive methods to disseminate information, may provide an initial means to counteract this issue.

The use of decision aids, such as external email banners and threat updates, was also highlighted as providing valuable assistance in drawing individuals' attention to potential risks when an email is first received. Once doubt has been invoked with regards to the legitimacy of the email, reporting mechanisms were highlighted as providing a means to verify suspicions and receive feedback on judgements. The consistent provision of such feedback was considered important to ensure that those who reported emails did not consider their actions to be a waste of time, and therefore would continue to use reporting mechanisms in the future. Whilst all personnel should have access to formal support mechanisms, access to the more informal processes that were highlighted, such as peer verification and support, is likely to be limited in certain staff groups (e.g., remote workers or those working off-site). As such, ensuring that all staff can access consistent technical feedback when required should be combined with a further consideration of potential options for supporting remote staff groups using informal online support tools, such as the development of specific internal forums or remote communication functions.

Finally, a number of perceived knowledge gaps also emerged that may impact susceptibility to spear phishing attacks. Specifically, these focused on (a) the degree of *understanding of the technical mechanisms* involved when a potential phishing email is responded to (e.g., when a malicious link is clicked on), (b) the *potential impact* of responding to such an email, including the likely trajectory of such impacts and how these impacts can be mitigated, and (c) the degree of *understanding of the limitations of technical solutions and security systems*, such as email filters, so that users perceive themselves as a vital component of such systems, in line with socio-technical approaches (Sasse et al., 2007). By empowering individuals with greater understanding of both the consequences of their potential actions and how these consequences can be mitigated at each stage, uncertainty regarding the phishing threat may be reduced (Ng et al, 2009; Tsai et al., 2016). Such approaches should also target understanding of how seemingly innocent information may be used in the development of a targeted phishing attack, such as providing the contact details of an employee to a social engineer or displaying information on social media. This knowledge is also directly applicable to a personal context, where employees may perceive themselves as more vulnerable due to increased exposure to a range of phishing and spear phishing emails and reduced availability of specialist support when deciding how to respond (Ng et al, 2009; Tsai et al., 2016).

The degree of technical knowledge that an individual has regarding the vulnerabilities of technical systems may also impact their understanding of the importance of human users as a secondary line of defence, and therefore their perceptions of both susceptibility and responsibility with regards to spear phishing (Ng et al, 2009; Tsai et al., 2016; Vishwanath et al., 2016). By focusing on the development of collaboration with security in order to achieve mutual goals (i.e., to reduce the phishing threat), uncertainties regarding the role and operations of security functions may be reduced and a greater understanding of the vulnerabilities of security systems developed. Consideration should also be given regarding how knowledge of these areas can be encouraged via other means, such as through the design of current system interfaces that may communicate this information in a visual manner at the time that the user interacts with an email.

4.3. Limitations and future work

It should be considered that this paper only reflects data from two organisations, and therefore further work is required to build on these findings and explore the extent that they are reflected in other organisations. This is particularly relevant for the findings of Study Two, since employee perceptions and experiences are likely to be impacted by a range of factors that may be specific to the organisation studied. Secondly, the extent that these perceptions reflect actual employee behaviour when faced with a spear phishing email would also benefit from further investigation in a more controlled setting. However, a number of factors identified relate directly to susceptibility concepts that have previously been examined in laboratory settings or using university populations. Thirdly, it should be noted that recruitment to the focus groups was based on voluntary participation, which could have skewed the sample to employees who were more knowledgeable or had a greater interest in this area. However, a wide range of awareness and knowledge levels and opinions related to phishing was demonstrated in discussions.

Finally, the use of historic phishing simulation data in Study One represents a novel approach in exploring phishing susceptibility in applied settings and provides a unique method for exploring the impact of message-related factors on response behaviour. However, this meant that it was not possible to counterbalance the particular influence techniques used within phishing emails, making it more difficult to assess these factors as individual constructs. Similarly, it was not possible to access demographic data regarding respondent attributes (e.g., age, cyber security knowledge, job role etc.). The availability of only nine simulated phishing emails also reduced the number of influence techniques that could feasibly be examined. Therefore, although this study focused on the impact of only two influence techniques (authority and urgency), future work should explore the potential role of other influence techniques and message-related factors, such as the time of day that an email is received, in impacting susceptibility within the workplace.

Future work exploring the extent to which employees divulge confidential information (e.g., usernames and passwords) after clicking on a link would also be beneficial to explore when people may become suspicious of attempts to elicit information. However, whether people click on malicious links alone, and how to reduce this, is still of interest to organisational security personnel. Overall, the use of such data represents a novel approach in exploring spear phishing susceptibility in applied settings, and we believe that it provides a unique method for exploring the impact of message-related factors on response behaviour, which we hope will be built upon in future work.

4.4. Conclusions

In sum, the findings of our study highlight the importance of considering the wider work context in relation to employee susceptibility to both spear phishing emails and phishing in general. Work-based norms and routines likely represent a primary factor impacting response behaviour within the workplace, influencing the development of context-specific habits, expectations and perceptions of risk. These are all likely to influence the information processing strategies that are used when a suspicious email is encountered and its resultant success. Reflective of the combined findings of Study One and Two, considering aspects of the email that is received, the individual who receives it, and the context in which it is encountered, within theoretical approaches is vital if susceptibility within the workplace is to be truly understood. It is hoped that the findings of the current study will provide a basis for further theoretical development in this field, whilst also presenting an initial aid for user communities to consider, and begin to address, the range of potential susceptibility factors that may be present within organisational settings.

Funding

This work was part funded by the Centre for Research and Evidence on Security Threats (ESRC award: ES/N009614/1).

Declarations of interest

None.

References

Abawajy, J., 2014. User preference of cyber security awareness delivery methods. Behav. Inf. Secur. 33 (3), 237–248.
Akbar, N., 2014. Analysing Persuasion Principles in Phishing Emails. Masters Thesis. University of Twente. Retrieved from http://essay.utwente.nl/66177/1/Akbar_MA_EEMCS.pdf on 6th October 2016.
Atkins, B., Huang, W., 2013. A study of social engineering in online frauds. Open J. Soc. Sci. 1, 23–32. https://doi.org/10.4236/jss.2013.13004.
Barnett, J., Breakwell, G.M., 2001. Risk perception and experience: Hazard personality profiles and individual differences. Risk Anal. 21 (1)), 171–178.
Begg, I.M., Anas, A., Farinacci, S., 1992. Dissociation of processes in belief: source recollection, statement familiarity, and the illusion of truth. J. Exp. Psychol. 121 (4)), 446–458. https://doi.org/10.1037/0096-3445.121.4.446.
Berg, B.L., 2006. Qualitative Research Methods for the Social Sciences, sixth ed. MA: Allyn & Bacon, Boston.
Bromiley, P., Curley, S.P., 1992. Individual differences in risk taking. In: Yates, F.J. (Ed.), Risk-Taking Behavior. John Wiley & Sons, Oxford, England, pp. 87–132.
Butavicius, M., Parsons, K., Pattinson, M., McCormac, A., 2015. Breaching the human firewall: social engineering in phishing and spear phishing emails. In: Australasian Conference on Information Systems.
Canfield, C.I., Fischhoff, B., Davis, A., 2016. Quantifying phishing susceptibility for detection and behavior decisions. Hum. Factors 58 (8), 1158–1172.
Caputo, D.D., Pfleeger, S.L., Freeman, J.D., Johnson, M.E., 2014. Going spear phishing: exploring embedded training and awareness. IEEE Secur. Privacy 12 (1), 28–38. https://doi.org/10.1109/MSP.2013.106.
Cialdini, R., 2007. Influence: The psychology of Persuasion. HarperCollins, New York.
Computer Fraud & Security, 2016. News - employees prone to phishing. Comput. Fraud Secur. 1, 3. https://doi.org/10.1016/S1361-3723(16)30004-5.
Conway, D., Taib, R., Harris, M., Yu, K., Berkovsky, S., Chen, F., 2017. A qualitative investigation of bank employee experiences of information security and phishing. In: Proceedings of the Thirteenth Symposium on Usable Privacy and Security, SOUPS '17.
Dewey, M.E., 1983. Coefficients of agreement. Br. J. Psychiatry 143, 487–489.
Dodge, R.C., Carver, C.A., Ferguson, A.J., 2007. Phishing for user security awareness. Comput. Secur. 26 (1), 73–80.
Downs, J., Holbrook, M., Cranor, L., 2006. Decision strategies and susceptibility to phishing. In: Symposium on Usable Privacy and Security, Pittsburgh, PA, pp. 79–90. https://doi.org/10.1145/1143120.1143131.
Eagly, A.H., Chaiken, S., 1993. The Psychology of Attitudes. Harcourt Brace Jovanovich College Publishers, San Diego, CA.
Fereday, J., Muir-Cochrane, E., 2006. Demonstrating rigor using thematic analysis: a hybrid approach of inductive and deductive coding and theme development. Int. J. Qual. Methods 5 (1), 80–92.
Grill-Spector, K., Henson, R., Martin, A., 2006. Repetition and the brain: neural models of stimulus-specific effects. Trends Cogn. Sci. 10 (1), 14–23. https://doi.org/10.1016/j.tics.2005.11.006.
Harrison, B., Svetiieva, E., Vishwanath, A., 2016a. Individual processing of phishing emails: how attention and elaboration protect against phishing. Online Inf. Rev. 40 (2), 265–281.
Harrison, B., Vishwanath, A., Rao, R., 2016b. A user-centred approach to phishing susceptibility: the role of a suspicious personality in protecting against phishing. In: 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, 5–8 January, pp. 5628–5634.

Hodgetts, H.M., Jones, D.M., 2006. Interruption of the tower of London task: support for a goal-activation approach. J. Exp. Psychol. 135 (1), 103–115. https://doi.org/10.1037/0096-3445.135.1.103.

INFOSEC Institute, 2013. Phishing Techniques, Similarities, Differences and Trends – Part II: Targeted Phishing. INFOSEC Institute Resources Accessed from. http://resources.infosecinstitute.com/phishing-techniques-similarities-differences-and-trends-part-ii-targeted-phishing/.

Irvine, P., Anderson, K., 2006. Collective information practice: exploring privacy and security as social and cultural phenomena. Hum. Comput. Interact. 21, 319–342. https://doi.org/10.1207/s15327051hci2103_2.

Kahneman, D., 2011. Thinking, Fast and Slow. Penguin, London, UK.

Kahneman, D., 1973. Attention and Effort. Prentice-Hall, Englewood Cliffs, NJ Prentice-Hall.

Kainda, R., Flechais, I., Roscoe, A.W., 2010. Security and usability: analysis and evaluation. In: Fifth International Conference on Availability, Reliability and Security (ARES 2010), 15–18 February 2010, Krakow, Poland.

Kirwan, B., Ainsworth, L., 1992. A Guide to Task Analysis. Taylor and Francis, London, UK.

Landesman, T., 2016. 55 companies and counting – W-2 spear phishing attacks continue to increase. Cloudmark Security Blog. accessed on 25.07.2016 at. https://blog.cloudmark.com/2016/03/31/55-companies-and-counting-w-2-spear-phishing-attacks-continue-to-increase/.

Luo, X., Zhang, W., Burd, S., Seazzu, A., 2013. Investigating phishing victimization with the Heuristic-systematic model: a theoretical framework and an exploration. Comput. Secur. 38, 28–38.

Miarmi, L., DeBono, K.G., 2007. The impact of distractions on heuristic processing: internet advertisements and stereotype use. J. Appl. Soc. Psychol. 37 (3)), 539–548. https://doi.org/10.1111/j.1559-1816.2007.00173.x.

Modic, D., Anderson, R.J., 2014. Reading this may harm your computer: the psychology of malware warnings. Comput. Hum. Behav. 41, 71–79. https://doi.org/10.1016/j.chb.2014.09.014.

National Cyber Security Centre, 2018. The trouble with phishing. Accessed on 26.03.2018 at https://www.ncsc.gov.uk/blog-post/trouble-phishing.

National Cyber Security Centre, 2018. Phishing attacks: defending your organisation. Accessed on 19.04.2018 at https://www.ncsc.gov.uk/phishing.

Ng, B-Y., Kankanhalli, A., Xu, Y., 2009. Studying users' computer security behaviour: a health belief perspective. Decis. Support Syst. 46, 815–825. https://doi.org/10.1016/j.dss.2008.11.010.

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, D., Lin, T., Ebner, N., 2017. Dissecting spear phishing emails for older vs young adults: on the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, CHI '17, pp. 6412–6424.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., Butavicius, M., 2012. Why do some people manage phishing emails better than others? Inf. Manage. Comput. Secur. 20 (1), 18–28. https://doi.org/10.1108/09685221211219173.

PhishMe, 2016. Enterprise Phishing Susceptibility Report. Accessed on 30.01.2017 at. https://phishme.com/project/enterprise-phishing-susceptibility-report/.

Piggin, R., 2016. Cyber security trends: what should keep CEOs awake at night. Int. J. Crit. Infrastruct. Prot. 13, 36–38. https://doi.org/10.1016/j.ijcip.2016.02.001.

Polage, D.C., 2012. Making up history: false memories of fake news stories. Europe's J. Psychol. 8 (2), 245–250. https://doi.org/10.5964/ejop.v8i2.456.

Rocha-Flores, W., Ekstedt, M., 2016. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Comput. Secur. 59, 26–44.

Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change. J. Psychol. 91, 93–114.

Sasse, M.A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Fléchais, I., Kearney, P., 2007. Human vulnerabilities in security systems. Human Factors Working Group White Paper, Cyber Security Knowledge Transfer Network.

Sasse, M.A., Brostoff, S., Weirich, D., 2001. Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security. BT Technol. J. 19 (3), 122–131.

Sivaramakrishnan, S., Manchanda, R.V., 2003. The effect of cognitive busyness on consumers' perceptions of product value. J. Prod. Brand Manage. 12 (5), 334–345. https://doi.org/10.1108/10610420310491693.

Stajano, F., Wilson, P., 2011. Understanding scam victims: seven principles for systems security. Commun. ACM 54 (3), 70–75. https://doi.org/10.1145/1897852.1897872.

Sun, J.C-Y., Yu, S-J., Lin, S.S.J., Tseng, S-S., 2016. The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. Comput. Hum. Behav. 59, 249–257.

Taylor, S.E., Fiske, S.T., 1978. Salience, attention, and attribution: top of the head phenomena. Adv. Exp. Soc. Psychol. 11, 249–288. 10.1016/S0065-2601(08)60009-X.

ten Brinke, L., Vohs, K.D., Carney, D.R., 2016. Can ordinary people detect deception after all? Trends Cogn. Sci. 20 (8), 579–588. https://doi.org/10.1016/j.tics.2016.05.012.

Tsai, H.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J., Cotton, S.R., 2016. Understanding online safety behaviors: a protection motivation theory perspective. Comput. Secur. 59, 138–150. https://doi.org/10.1016/j.cose.2016.02.009.

Verizon, 2016. 2016 Data Breach Investigations Report. Accessed on 23.09.2016 at. http://www.verizonenterprise.com/verizon-insights-lab/dbir/.

Vishwanath, A., 2015. Examining the distinct antecedents of email habits and its influence on the outcomes of a phishing attack. J. Comput. Mediated Commun. 20 (5), 570–584.

Vishwanath, A., Harrison, B., Ng, Y.J., 2016. Suspicion, cognition, and automaticity model of phishing susceptibility. Commun. Res. 1–21. https://doi.org/10.1177/0093650215627483. online pre-print.

Vishwanath, A., Herath, T., Chen, R., Wang, J., Rao, H.R., 2011. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decis. Support Syst. 51, 576–586. https://doi.org/10.1016/j.dss.2011.03.002.

Vohs, K.D., Baumeister, R.F., Schmeichel, B.J., Twenge, J.M., Nelson, N.M., Tice, D.M., 2008. Making choices impairs subsequent self-control: a limited-resource account of decision making, self-regulation, and active initiative. J. Pers. Soc. Psychol. 94 (5), 883–898. https://doi.org/10.1037/0022-3514.94.5.883.

Wang, J., Li, Y., Rao, R., 2017. Coping responses in phishing detection: an investigation of antecedents and consequences. Inf. Syst. Res. 28, 378–396.

Williams, E.J., Beardmore, A., Joinson, A., 2017a. Individual differences in susceptibility to online influence: a theoretical review. Comput. Hum. Behav. 72, 412–421.

Williams, E.J., Morgan, P., Joinson, A., 2017b. Press accept to update now: individual differences in susceptibility to malevolent computer updates. Decis. Support Syst. 96, 119–129.

Woolley, A., Chabris, C.F., Pentland, A., Hashmi, N., Malone, T.W., 2010. Evidence for a collective intelligence factor in the performance of human groups. Science 330 (6004), 686–688. https://doi.org/10.1126/science.1193147.

Workman, M., 2008. Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security. J. Am. Soc. Inf. Sci. Technol. 59 (4), 662–674. https://doi.org/10.1002/asi.20779.

Wright, R.T., Jensen, M.L., Thatcher, J.B., Dinger, M., Marett, K., 2014. Research note - influence techniques in phishing attacks: an examination of vulnerability and resistance. Inf. Syst. Res. 25 (2), 385–400.

Zetter, K., 2016. Inside the cunning, unprecedented hack of Ukraine's power grid. WIRED. accessed on 25.07.2016 at https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.